UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

-against-

JACOB DELANEY,

Defendant.

REPLY BRIEF

O'CONNELL AND ARONOWITZ
Attorneys for Defendant
54 State Street
Albany NY 12207-2501
(518) 462-5601

SCOTT W. ISEMAN, ESQ.
Of Counsel

Dated: March 5, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Federal Cases

INTRODUCTION

The Defendant offers this memorandum of law in Reply to the Government's Response Brief in Opposition to the Defendant's Motion to Suppress. All references to Exhibits refer to the exhibits in Defendant's main motion.

ARGUMENT

I. The totality of the circumstances does not support probable cause

The Government's response does nothing to solve the following threshold deficiency in SA Fallon's warrant application: that based on SA Fallon's own representations, the Government is only guessing whether the Defendant's IP address was used by the actual target user who accessed the Target Site referenced by the FLA or if the Defendant's IP address was the exit node of a Tor relay used by the true target user. SA Fallon created this issue by affirming that:

- "due to the anonymity provided by the Tor network, it can be **difficult or impossible to determine**, at the beginning of an investigation, where in the world a particular website or user is located." *See* Ex. E to Iseman Dec. at ¶ 19. (under seal) (emphasis supplied).

- "[w]hen a TOR user accesses an Internet website, **only the IP address of the last relay computer (the "exit node") as opposed to the TOR user's actual IP address**, appears on the website's IP log." *Id.*at ¶ 11. (emphasis supplied).

- "Because of the way the Tor network routes communications through the relay computers, **traditional IP address identification techniques are not effective**." *Id*. at ¶ 8. (emphasis supplied).

Neither the FLA, SA Fallon's application, nor the Government's response clarify the central issue in this case: How does the Government establish that the Defendant's IP address was used by the actual target user to access the Target Site?

The Government does not describe any method for actually identifying the target user of a Tor browser. Instead, it only offers that it is reasonable to assume from the totality of the circumstances that the FLA employed "some lawful investigative technique that allowed it to identify the Tor user accessing the Target website." (Gov. Opp. Brief at 11). Based on SA Fallon's representations, however, the FLA's undescribed "lawful technique", would also have to be a "non-traditional" IP address identification technique that somehow identified a specific IP address in the United States entirely from overseas when such determinations can be "impossible" to make. (*Cf Id.* with Ex. "E" to Iseman Dec. at ¶¶ 8 and 21; *See also* Ex. "D" to Iseman Dec. at 3 "there is no practical method to trace a user's actual IP address back through those Tor relay computers."). This is conjecture, not a reasonable inference from the totality of the circumstances provided to the reviewing Magistrate.

Quite the opposite, since the **only** information the Government provides about how IP addresses operating on Tor browsers can be tracked is that "[w]hen a TOR user accesses an Internet website, **only the IP address of the last relay computer (the "exit node") as opposed to the TOR user's actual IP address**, appears on the website's IP log" (Ex. "E" to Iseman Dec. at ¶ 8), the totality of the circumstances requires the conclusion that the target IP address identified by the FLA is the exit node's, not the actual Tor user's IP address. (emphasis supplied). The Government should not be able to ignore the significance of its own sworn statements by relying on a hopeful train of inferences and imputed knowledge that directly contradicts what its own agent affirms under oath. It is obvious based on SA Fallon's representations about the meddlesome nature of Tor that more investigation was required by the Government to determine whether the Defendant's IP address was the target user, the exit node or some intermediary relay before the Government could obtain probable cause to search his residence.

The ability to pursue such corroborative investigative information was available to the Government since the referral to the Albany Field Office included an application for a pen register/trap and trace pony (PRTT Pony), which is "effective in determining whether Tor network traffic is coming from a residence." *See* Ex. "D" to Iseman Dec. (under seal). The Government's response makes no mention of why it did not apply for PRTT Pony.

Relatedly, the Government relies heavily on the hidden nature of the Target Site and the multiple affirmative steps that SA Fallon affirmed are necessary to access the Target Site as evidence of the target user's predisposition to collect child pornography. Gov. Opp. Brief at 4-5, 9-10, 13-14. In short, the Government argues that the target user going to the target site is "no mere happenstance". *Id*. at 13. But this point is also directly undermined by SA Fallon's own claims since he provides a perfectly reasonable explanation for how it may **appear** like a user at a specific IP address accessed the Target Site when, in fact, they did not. SA Fallon affirmed that "[w]hen a TOR user accesses an Internet website, only the IP address of the last relay computer (the "exit node") as opposed to the TOR user's actual IP address, appears on the website's IP log." *Id.* As a result, simply by having a Tor browser, an individual's IP address can access the Target Site as the exit node for **another** Tor user. That is why the exit node's IP address, as opposed to the "TOR user's actual IP address" would appear on "the [target website's] IP log." Ex. "E" to Iseman Dec. at ¶ 11. The Government cannot escape this reality.

II. The Government disregards the importance of *Raymonda*

The Government makes no effort to distinguish this matter from *Raymonda* because it cannot.[1] *United States v. Raymonda*, 780 F.3d 105 (2d Cir. 2015). *Raymonda* requires in cases

[1] Notably, while the Government represents (without transcript, Affidavit or Declaration) that *United States v. Martin*, 426 F.3d 68 (2d Cir. 2005) and *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) were considered by the reviewing Magistrate, *Raymonda* apparently was not. *See* Gov. Opp. Brief at 17, Note 8.

where a warrant application alleges only one, months old, point of access to a site affiliated with child pornography, that more is needed to establish probable cause than a single instance of access to a contraband site. *Id*. at 115 (more is needed since "such circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged."). What qualified as "more" is not elusive. As described below, in each of the cases cited by the Second Circuit as examples of where additional evidence was found to overcome staleness and sufficiency concerns, the search warrant affidavits provided evidence of specific **additional affirmative acts** beyond accessing the suspect site. *Id*. For example, in *United States v. Vosburgh*, the affidavit established the suspect accessed a contraband site and attempted to download a contraband video three separate times. 602 F.3d 512, 518 (3d Cir. 2010). In *United States v. Hay*, the affidavit contained evidence that 19 contraband files were separately downloaded. 231 F. 3d 630, 634 (9th Cir. 2000). Finally, in *United States v. Seiver*, the affidavit contained evidence that the suspect both downloaded a contraband video and uploaded multiple contraband images to the site. 692 F.3d 774. 775-77 (7th Cir. 2012). The affidavit here contains no similar affirmative acts or even an act.

It is also noteworthy that the search warrant affidavit in *Raymonda* contained substantially more allegations of affirmative conduct by the suspect including a claim that the suspect accessed 76 separate images and "'more than one incidence of access of thumbnail [contraband] images by the user'". *Id*. at 110. While the agent's representations of affirmative conduct by the suspect were largely discredited (*Id*. at 111-12) the Government does not even try to make similar representations here about the target user's affirmative conduct on the Target Site. The Government cannot do so here because it has no such evidence.

At the same time, the Government overstates the import of *United States v. Martin*, 426 F. 3d 68 (2d Cir. 2005).[2] *Martin* turned on the suspect's deliberate registration for membership in an internet group devoted to the distribution of child pornography. *Martin*, 426 F.3d at 73. This was an affirmative act that showed a demonstrable interest in child pornography. While SA Fallon detailed the awful things a registered user of the Target Site could do, he never affirmed that anyone using the target IP address or that the Defendant was a registered user or any similar affirmative act for an inference to be drawn that evidenced a demonstrable interest in child pornography.

Even if it is accepted that the target user is somehow linked to the Defendant's IP address, there is still no evidence other than the use of a Tor browser and a single instance of access that occurred more than seven months earlier. And the use of the Tor browser is not enough. The Government needed to establish like in *Vosburgh*, *Hay*, and *Seiver*, *supra,* some evidence that the target user took affirmative action related to the contraband. But there is no evidence of a click, a log in, a username, a download, an upload, a post, a request, a purchase, or an exchange that infers more than a mere "brush" with child pornography. *Raymonda*, 780 F.3d at 115. Since the warrant application fails to do so here, it fails to establish probable cause under clearly established Second Circuit law.

III. The Government improperly relies on *United States v. Sanders*

The Government relies heavily on *United States v. Sanders* and this reliance is improper since the underlying facts of the case are largely sealed at the Government's request. 1:20-cr-00143 (TSE) (Dkt. No. 122). While the decision itself is largely unredacted, the search warrant

[2] It should also be noted that *Martin* is on best, shaky ground. In *United States v. Coreas,* 419 F.3d 151 (2d Cir. 2005), a different Second Circuit panel expressed that *Martin* was wrongly decided but yielded to it because it was heard first.

application and other relevant materials related to it are sealed. (*see* Dkt. No. 28, Protective Order).[3] As a result, the Defendant has no way to compare and contrast SA Fallon's application with the sufficiency of the warrant application in *Sanders*. The Government is the only entity in a position to makes these comparisons and appreciate their application to this case.[4]

From what can be gleaned from the publicly available information in *Sanders*, it appears that the Defendant there did not make a similar factual deficiency argument related to Tor frustrating law enforcement's ability to distinguish between an actual user and an intermediary relay on the Tor network as is made here. What other distinctions may exist are speculative. As a result, the Court should disregard this portion of the Government's argument.

IV. The Government is not entitled to the good faith exception

Raymonda and *Falso* control the probable cause analysis for this matter and these decisions have been well established for years prior to the warrant application here. The existence of a Tor browser and purported steps needed to access the Target Site do not sufficiently distinguish this matter from *Raymonda* and *Falso* such that the Government gets a constitutional pass – particularly when the applying agent's representations actively contradict his own conclusions about there being a direct connection between the target IP address and the Target Site. *United States v. Clark*, 638 F.3d 89, 105 (2d Cir. 2011) (law enforcement cannot "claim reasonable reliance on warrants secured in the absence of compliance" with clearly established law).

[3] Notably defense counsel in *Sanders* attempted to modify the protective order to permit sharing of the search warrant and other related materials with other defense counsel involved in the same investigation. *Sanders*, Dkt. No. 229. The Court denied that motion. (*Id*. Dkt. No. 257)

[4] Defense counsel conferred with the Government Counsel on this issue by phone and email and requested that the Government withdraw its arguments on *Sanders* or take the steps necessary to unseal the underlying exhibits to afford the defense an opportunity to fully compare the facts underlying the court's decision. After considering the Defense's request, the Government refused. The Defendant acknowledges that Government Counsel on this matter does not have personal knowledge or access to any additional information in *Silver* than the Defense. Nonetheless, the United States Government does.

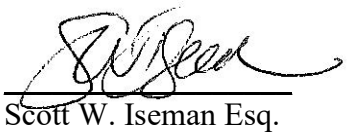
Similarly, the Defendant agrees that a *Franks* hearing is not necessary as there is no issue of fact that needs resolution or amplification from an evidentiary hearing. The Defendant is not and has not made any claim that SA Fallon **intentionally** mislead the court, only that he was reckless in his application by ignoring well established controlling law as described above and not including anywhere near the facts necessary to establish probable cause. Relatedly, the Government is not entitled to the good faith exception when it does not share all "potentially adverse information" to the reviewing Magistrate. *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.), *on reh'g*, 91 F.3d 331 (2d Cir. 1996). Here, the Government failed to disclose that the Defendant's IP address was not registered with the National Center For Missing and Exploited Children ("NCMEC") or the ICAC Child Online Protection System; that the Defendant had no prior criminal history, was not a registered sex offender, and FBI database searches "did not identify any derogatory information" about the Defendant. Ex. "D" to Iseman Dec. at pg. 4-5. Since none of this information (which is adverse to the SA Fallon's representation that a the Defendant was linked to a child sexual exploitation website) was made known to the court, the Government does not get the benefit of the good faith exception.

CONCLUSION

For the above reasons, the Defendant respectfully requests that the Court suppress all evidence seized during the search of the Defendant's apartment and any statement made by Defendant to law enforcement on December 12, 2019.

Dated: Albany, New York
March 5, 2021

O'CONNELL & ARONOWITZ P.C.

By: 

Scott W. Iseman Esq.
Attorney for Plaintiff
Bar Roll No.: 518859
54 State Street, 9th Floor
Albany, NY 12207
(518) 462-5601
siseman@oalaw.com